Application No. 10826435 (Docket: CNTR.2075)
37 CFR 1.111 Amendment dated 03/07/2008
Reply to Office Action of 12/11/2007

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0020.1] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a fetch logic, translation logic, and execution logic. The fetch logic is disposed within a microprocessor, and is configured to receive a cryptographic instructionsingle atomic cryptographic instruction as part of an instruction flow executing on the microprocessor. The cryptographic instructionsingle atomic cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that an intermediate result be generated. The translation logic is coupled to the fetch logic, and is configured to translate the single atomic cryptographic instruction into a sequence of micro instructions that directs the microprocessor to perform the one of the cryptographic operations. The execution logic is disposed within the microprocessor and is operatively coupled to the cryptographic instructionsingle atomic cryptographic instruction. The execution logic executes the one of the cryptographic operations, and generates the intermediate result. The execution logic includes a cryptography unit that is configured execute a plurality of cryptographic rounds on each of one or more input text blocks to generate a corresponding each of one or more output text blocks, where the plurality of cryptographic rounds are prescribed by a round count field within a control word that is provided to the cryptography unit.

[0021] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a control word and a cryptography unit. The control word prescribes that an intermediate result be generated during execution of one of the cryptographic operations. The cryptography unit is disposed within execution logic in within a microprocessor and is configured to execute the one of the cryptographic

Application No. 10826435 (Docket: CNTR.2075)
37 CFR 1.111 Amendment dated 03/07/2008
Reply to Office Action of 12/11/2007

operations responsive to receipt of a ~~cryptographic instruction~~single atomic cryptographic instruction within an instruction flow that prescribes the one of the cryptographic operations, where the ~~cryptographic instruction~~single atomic cryptographic instruction is fetched from memory by fetch logic in the microprocessor, and where the ~~cryptographic instruction~~single atomic cryptographic instruction also references the control word. Translation logic in the microprocessor translates the single atomic cryptographic instruction into a sequence of micro instructions that directs the microprocessor to perform the one of the cryptographic operations.

[0022] Another aspect of the present invention provides a method for performing cryptographic operations. The method includes, within a microprocessor, fetching a ~~cryptographic instruction~~single atomic cryptographic instruction from memory prescribing that an intermediate result be generated during execution of one of a plurality of cryptographic operations; and, within the microprocessor. receiving the cryptographic ~~instruction~~single atomic cryptographic instruction. translating the single atomic cryptographic instruction into a sequence of micro instructions that direct the microprocessor to perform the one of the plurality of cryptographic operations, and via a cryptography unit disposed within execution logic in the microprocessor. generating the intermediate result when executing the one of the cryptographic operations.

Kindly replace paragraph [0012] with the following amended paragraph:

[0012] To perform cryptographic operations on multiple successive blocks of text, all of the symmetric key algorithms employ the same types of modes. These modes include electronic code book (ECB) mode, cipher block chaining (CBC) mode, cipher feedback (CFB) mode, and output feedback (OFB) mode. Some of these modes utilize an additional initialization vector during performance of the sub-operations and some use the ciphertext output of a first set of cryptographic rounds performed on a first block of plaintext as an additional input to a second set of cryptographic rounds performed on a second block of plaintext. It is beyond the scope of the present application to provide an in depth discussion of each of the cryptographic algorithms and sub-operations employed by present day symmetric key cryptographic algorithms. For specific implementation

Page 3 of 26

Application No. 10826435 (Docket: CNTR.2075)
37 CFR 1.111 Amendment dated 03/07/2008
Reply to Office Action of 12/11/2007

standards, the reader is directed to Federal Information Processing Standards Publication 46-3 (FIPS-46-3), dated October 25, 1999 for a detailed discussion of DES and Triple DES, and Federal Information Processing Standards Publication 197 (FIPS-197), dated November 26, 2001 for a detailed discussion of AES.   Both of the aforementioned standards are issued and maintained by the National Institute of Standards and Technology (NIST) and are herein incorporated by reference for all intents and purposes. In addition to the aforementioned standards, tutorials, white papers, toolkits, and resource articles can be obtained from NIST's Computer Security Resource Center (CSRC) over the Internet at http: 'csrc.nist.gov .